白皮书

微分段关键用例探讨

作者：Enterprise Strategy Group 高级分析师 John Grady

2023 年 1 月

Enterprise Strategy Group 发布的这份白皮书由 Akamai 委托撰写，经 TechTarget，Inc. 许可分发。

目录

要点概述

在网络安全行业中，Zero Trust 已无处不在。然而，该计划涉及范围极广，而且关于该战略的哪些方面最为重要还存在不少争议，因此对于从何处着手、哪些工具能为该框架提供最好的支持，人们还不甚明确。虽然实现 Zero Trust 没有统一途径，但该战略能否成功实施，最终取决于是否能确保资源和实体只有在获得策略明确允许的情况下才能相互通信，这也彰显了微分段的重要性。

目前，微分段工具的使用受到一定程度的限制，但一旦人们认识到微分段对 Zero Trust 的重要性及其在各种用例中的适用性，预计情况会大有改善。无论企业是考虑采用 Zero Trust 来防范威胁并提高整个企业的效率，还是实现其整体安全方法的现代化，微分段都可以提供帮助。特别是 Akamai 基于软件且受到人工智能支持的微分段方法提供了精细的监测能力，允许企业在整个环境中始终如一地阻止横向移动、抵御勒索软件攻击并实施 Zero Trust 原则。

无论企业是考虑采用 Zero Trust 来防范威胁并提高整个企业的效率，还是实现其整体安全方法的现代化，微分段都可以提供帮助。

Zero Trust 获得广泛认可，但关键是要确立明确的优先事项

随着资源向云倾斜、数字业务模式成为主流以及用户日益分散，企业环境的复杂性也在不断增加。随着攻击者试图利用防御漏洞发起勒索软件攻击、窃取客户信息或外泄敏感的知识产权，这些变化本身会加大网络安全团队的工作难度。遗憾的是，传统安全方法依赖于过度宽松的边界式控制，而这已经不足以应对当今的现实情况，因此安全团队不得不重新评估其策略。此外，攻击数量和复杂性也在不断增加，安全团队无法跟上攻击的变化速度，难以解决每个潜在威胁并予以修补。

这些问题促使许多企业开始探索 Zero Trust 的概念。Zero Trust 战略并不是新鲜概念，却吸引了众多企业的高度关注，并被视为一种更加动态、可保持最小访问权限和基于风险的网络安全保护方法。Zero Trust 方法消除了数字环境中的隐性信任，并且会始终如一地验证每一次数字互动。所以，Zero Trust 方法应该能让安全团队更有信心地确保其资源、用户和设备的安全性和可用性。但也正是由于 Zero Trust 的广泛适用性，再加上人们对到底什么是 Zero Trust 的看法和定义有时存在冲突，这不但造成了困惑，也让企业难以决定从何处着手。

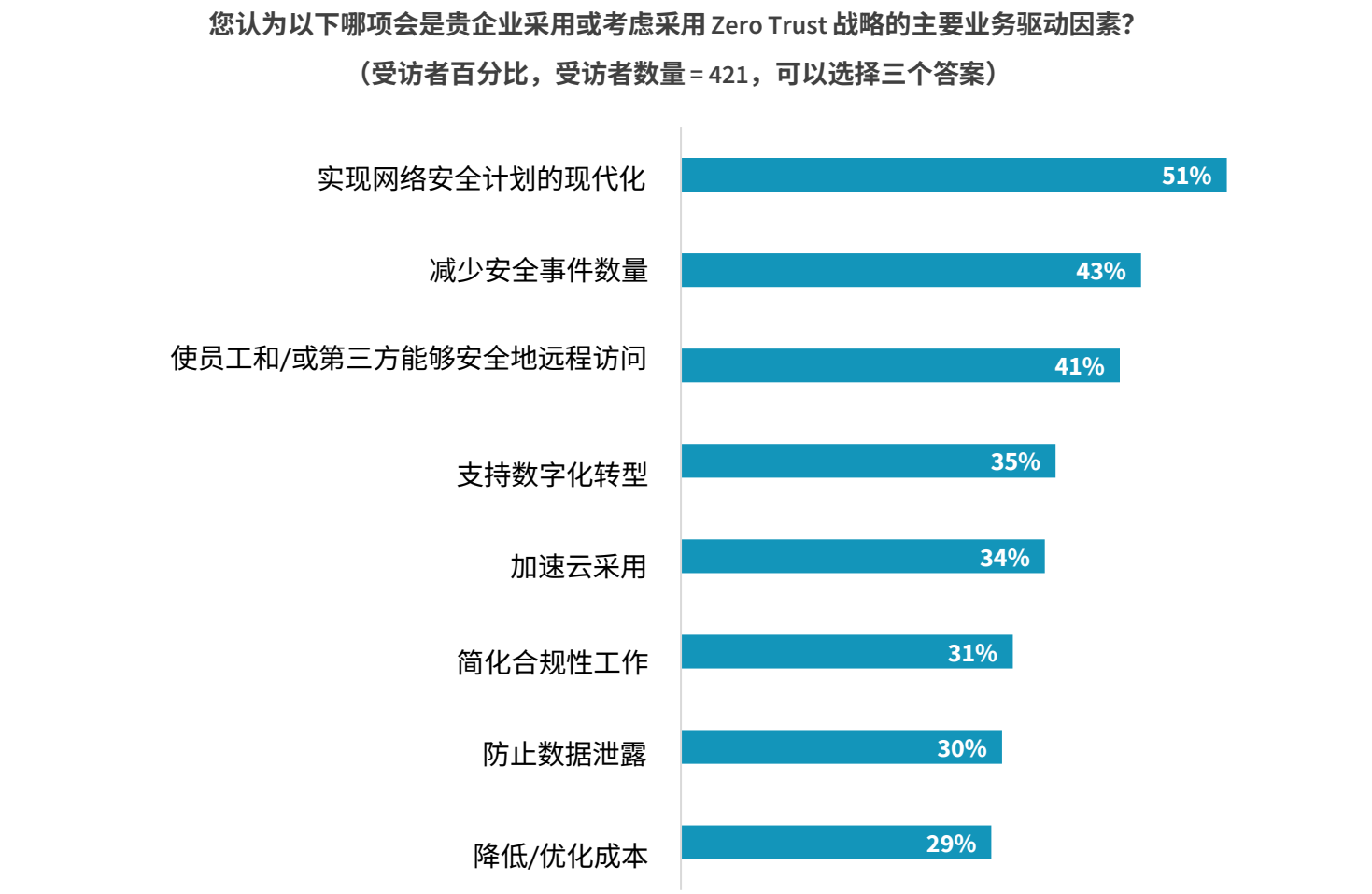
对企业优先事项和需要达到的结果进行评估有助于缩小重点范围，也有助于确定从何处着手实施 Zero Trust 计划。有多种业务因素推动着企业实施 Zero Trust 战略（参见图 1）。[1]最常见的目标是网络安全现代化，有 51% 的受访者提到这一点。拜登政府发布的网络安全行政命令在其现代化要求中提出了 Zero Trust 架构的概念，充分说明了美国联邦政府对这种思维模式的重视。这些命令虽然不是直接针对私营部门，却有助于为联邦政府以外的安全团队提供指导。Zero Trust 的其他战略目标还包括支持数字

Zero Trust 战略能否成功实施，取决于能否确保资源和实体只有在获得策略明确允许的情况下才能相互通信。

[1]资料来源：Enterprise Strategy Group 调查结果，*"The State of Zero Trust Security Strategies"*（Zero Trust 安全战略现状），2021 年 5 月。

化转型 (35%) 和加速云采用 (34%)。这些驱动因素凸显出一点：许多企业都希望安全团队能够帮助为业务赋能，而不仅仅是保护资产。还有一些更具战术意义的目标也比较普遍，例如减少安全事件数量 (43%)、实现安全远程访问 (41%)、简化合规性工作 (31%) 和防止数据外泄 (30%)。

图 1.采用 Zero Trust 的驱动因



资料来源：TechTarget, Inc. 下属 Enterprise Strategy Group 部门

在某些情况下，如果能够在一开始就缩小 Zero Trust 项目的重点范围，无疑能帮助安全团队确定支持该战略所需的工具。例如，如果目标是改善员工和第三方的安全远程访问，则许多人会采用 Zero Trust 网络访问 (ZTNA)。对于这种情况，多重身份验证 (MFA) 等身份识别工具也能发挥作用。但是，某些驱动因素的技术要求可能还比较含糊，即使在缩小范围之后，许多企业仍然还有多个重点目标。在这样的情况下，企业必须确定哪些工具和实践能够支持各种用例和结果。

微分段目前在支持 Zero Trust 模型方面尚未得到充分利用

虽然实现 Zero Trust 没有统一途径，但该战略能否成功实施，最终取决于能否确保资源和实体只有在获得策略明确允许的情况下才能相互通信。这意味着对任何企业来说，Zero Trust 理念的关键要素都应该是确保资产能够正确分段的能力，从而帮助限制攻击得逞所造成的影响。这一点可能适用于网络安全现代化等比较广泛的目标，或是防止数据外泄等更有针对性的目标。

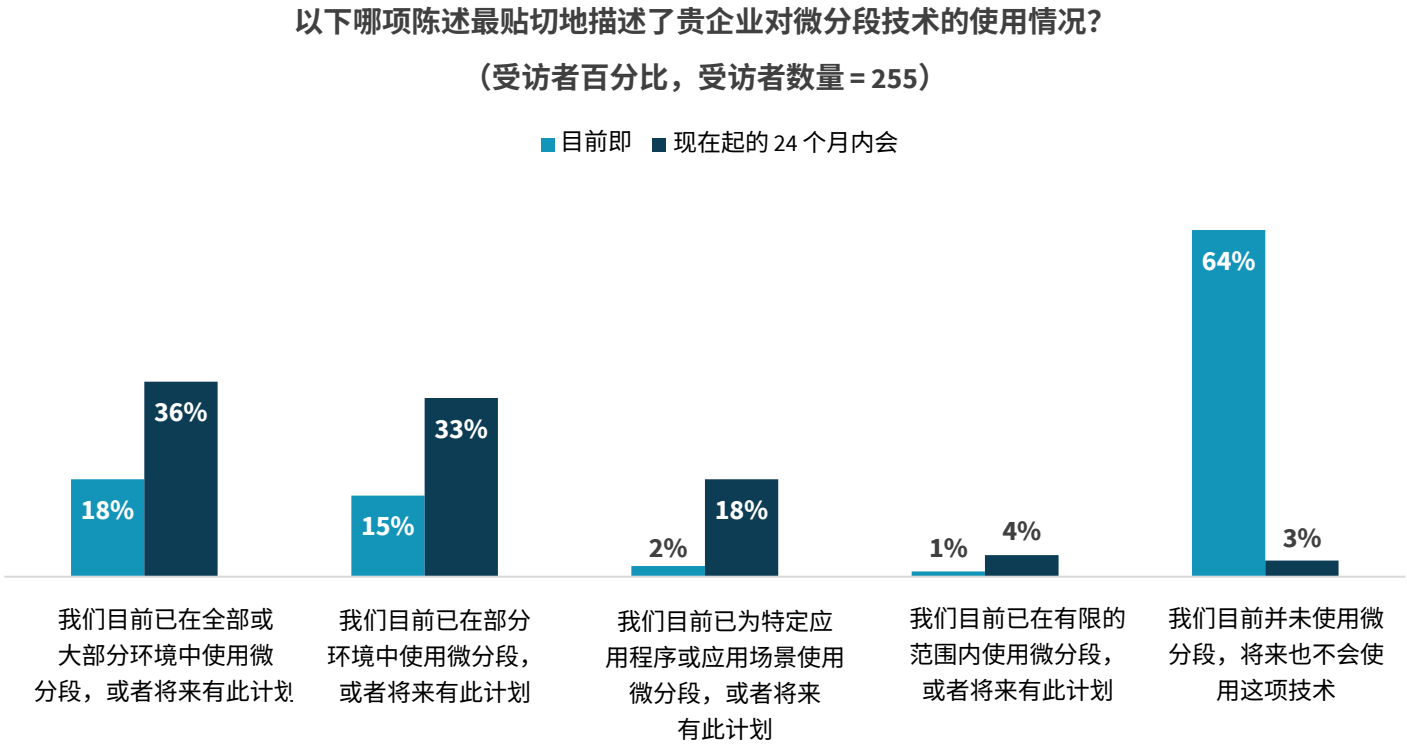
但在当下环境中，粗粒度的分段通常并不足够，需要更精细的微分段才能充分保护公司资产。现代应用程序架构通常依赖于分布在多个服务器实例中（某些情况下还包括分布在多个云环境中）的工作负载。按地点对资源进行分段的做法已经过时，无法解决安全团队如今所面临的挑战。

从历史上看，企业对微分段工具的采用历来较为犹豫。TechTarget Enterprise Strategy Group (ESG) 的研究发现，28% 的企业认为微分段过于复杂。但在很大程度上，这个问题可能源于安全团队使用了错误的工具来执行微分段。具体而言，ESG 研究发现，55% 的企业表示使用了基于基础架构的工具（例如防火墙）执行微分段，而只有 8% 的企业使用基于主机的工具。[2]防火墙无法强制实施成功微分段所需的精细化策略。此外，这些工具对应用程序工作负载的监测能力也很有限，难以做到在本地环境与云环境中一致地监测环境的所有方面。

这种情况导致微分段未能得到充分利用。尽管微分段对 Zero Trust 极其重要，但 ESG 研究发现，目前只有 36% 的企业采用了该技术（见图 2）。好消息是，许多企业都已经认识到自己在防御方面存在的这一重大缺口。因此，91% 的受访者预计将在 24 个月内采用微分段。[3]通过支持物理、虚拟和云网络抵御外部和内部威胁，微分段最终将巩固并增强 Zero Trust 的关键优势，并且应该成为任何 Zero Trust 战略的核心组成部分。

[2]资料来源：Enterprise Strategy Group 完整调查结果，*“Network Security Trends in Hybrid Cloud Environments”*（混合云环境中的网络安全趋势），2021 年 12 月。
[3]同前。

图 2.微分段的采用



资料来源：TechTarget, Inc. 下属 Enterprise Strategy Group 部门

微分段的关键用例

微分段广泛适用于各种 Zero Trust 用例，这也是它越来越受到重视的主要原因之一。但首先，微分段是开启 Zero Trust 之旅的良好起点，因为它可以确保企业最关键资产的安全性。如果使用的解决方案能够提供跨工作负载和实体关系的高精细度监测能力，成效将更为显著。流量和依赖关系基准的制定是任何 Zero Trust 工作的基础，也是在不中断业务的情况下消除隐性信任的第一步。这种方法允许安全团队快速实施最关键资产的保护，以帮助在 Zero Trust 实施过程中控制违规所造成的影响。有了这样的保障措施，安全团队便可以将注意力转向微分段支持的其他一些用例上。

预防威胁

Zero Trust 是一种安全性框架，而这种“安全性”的目的是保护企业免受网络威胁。因此，一些主要微分段用例的中心任务就是防范威胁并限制威胁对公司资源的影响，具体包括：

- **隔离关键资产。**安全团队在确定需要优先保护的对象时，必须对风险进行权衡。包含受监管客户信息、知识产权或其他敏感信息的高价值应用程序一旦遭到入侵，会造成更大的潜在影响，因此应该予以更多关注，也需要加强安全控制。通过采用微分段，安全团队可以确保这些应用程序及其所包含的工作负载与基础架构的其余部分完全分离。

- **限制横向移动。**Zero Trust 有一个原则未受到重视，那就是秉承“假设已被入侵”的思维模式，即假设攻击者能够访问公司网络。传统终端、服务器、云资源甚至智能设备不断增加，入侵在所难免。因此，通过实施微分段来限制潜在攻击的扩散范围，潜在攻击者便无法在网络中横向移动。

防范勒索软件

勒索软件依然猖獗，而且影响恶劣，因此已经引起高管层（甚至是董事会层面）的关注。勒索软件的应对准备不仅需要强大的安全性，还需要良好的数据保护和事件响应功能，而微分段可以帮助企业确保在抵御攻击方面打下扎实的基础。在攻击实施过程中，攻击者通常需要渗透环境并花时间进行侦察，然后才能将敏感信息和系统作为攻击目标。如果使用微分段来隔离关键资产并限制横向移动，攻击者在整个环境中移动的自由度就会降低。此外，一旦发现遭受勒索软件攻击，使用微分段的企业就可以快速关停攻击者使用的通信途径并隔离受感染的服务器，以防止攻击进一步扩散。

- **威胁检测和响应。**遭遇攻击时，企业必须分秒必争。微分段工具可以帮助安全团队快速有效地作出响应，让他们能够根据应用程序关系快速了解潜在的攻击途径、阻止攻击者在攻击期间使用的端口，并将受影响系统与网络的其余部分隔离开来。它还能控制对初始入侵点的攻击。

提高整个企业的效率

尽管安全团队的首要目标是保护数字环境，但受现状的限制，他们在实施保护的同时还不能影响业务效率。此外，如果安全团队能够切实为其同事赋能，业务部门也会因此而受益。这一点有诸多含义，其中一些最常见的包括：

- **支持云采用。**向云技术的转变并不是什么新鲜事物，但安全问题仍是许多企业最关心的因素。其中部分原因在于对基础架构即服务平台上的原生安全控制措施不够熟悉，另一部分原因是混合云环境中可能出现的安全措施不一致问题。微分段能让企业更有信心，因为它让企业能在其环境的所有方面应用控制措施，并且在混合云情景中实现更好的安全措施一致性。

- **助力应用程序现代化。**除了向云技术的转变之外，对容器等现代应用程序架构的采用也在不断加速。借助这些模式，应用程序团队能够比以往更快地设计、构建和部署应用程序。有了能够确保这些资源得到保护，并且不会限制开发人员工作速度的工具，就能对业务产生积极影响。微分段工具可以监测容器环境中的流量，并在容器联机或移动时自动应用分段策略，从而帮助开发团队确保其应用程序的安全。

- **简化合规性工作。**监管问题正在占用企业越来越多的时间、预算和注意力。确保尽可能隔离安全风险以限制潜在问题（例如，数据隐私泄露或个人身份信息丢失），就能大大减少此流程的繁琐程度。微分段可确保受合规要求约束的系统与环境的其余部分隔离开来，从而减轻安全团队的负担。

Zero Trust 分段

微分段最具吸引力的一个方面在于，它使企业能够专注于极具针对性的用例，从而立竿见影地为企业创造价值。对于许多人来说，其吸引力在于能够从迅速创造价值且相对比较容易处理的策略着手，例如制定访问拒绝名单、隔离关键应用程序、实施环境分段以及其他不太复杂的策略。很少有企业能够一次性完成整个微分段策略的全面部署。但是，随着 Zero Trust 计划范围内的微分段在整个环境中得到更广泛的部署，许多企业将开始采用 Zero Trust 分段方法。加上之前讨论的用例和积极成果，随着企业能够对流量进行全面且精细的监测、保护最敏感的资产、防止横向移动并且快速应对威胁，业务部门将获得更好的支持。虽然这并不是许多微分段项目的初衷，但应被视为一个长期目标。

Akamai 的微分段方法

Akamai Guardicore Segmentation 解决方案是一种基于软件的微分段方法，旨在阻止攻击者在数字环境中横向移动。

企业必须牢记，尽管微分段是 Zero Trust 的一个重要方面，但还有其他关键组成部分，需要采用其他技术来支持威胁检测和响应、身份识别、数据安全等。评估、选择技术供应商并与其开展合作是一个注重细节、讲究方法的过程，决定着企业能否实现其网络安全目标，同时避免浪费资金、时间和人力资源。因此，如果能够采用可提供广泛集成和信号共享功能的微分段工具，将有助于 Zero Trust 战略顺利迈进到微分段之外的领域，同时降低运营复杂性。

Akamai 长期深耕于网络基础架构领域，已将微分段和 Zero Trust 已成为其解决方案组合的核心部分。在本地环境与云环境的企业基础架构方面，该公司积累了丰富的经验，包括发现和应对潜在网络安全挑战的经验。

Akamai Guardicore Segmentation 是一种基于软件的微分段方法，旨在阻止攻击者在数字环境中横向移动。该解决方案利用精细监测，在网络层面上实施 Zero Trust 原则，帮助企业直观查看物理与虚拟环境中的活动和动向。其基于人工智能的分段框架使用集成的模板来发现和阻止入侵，例如勒索软件、基于终端的攻击以及针对远程员工的攻击。它适用于各种平台，包括裸机服务器、虚拟机、容器、物联网设备和云实例。

Akamai Guardicore Segmentation 通过多种方式收集有关底层基础架构的广泛数据，例如基于代理的传感器、基于网络的数据收集、虚拟私有云流量日志，以及可促进无代理功能的集成。动态映射让管理员能够获得粗粒度的端到端活动视图。凭借 Akamai 在企业网络环境方面积累的丰富经验，Akamai Guardicore Segmentation 专为实现企业可扩展性和一致的性能而设计，可从源头识别并避免流量瓶颈。

更重要的事实

微分段并不是一项新技术。实际上，它的出现可能提早了一个时代。但是，微分段的重要性毋庸置疑，它不但能保护现代混合型多云环境，更有助于实施 Zero Trust 战略。微分段提供了在许多关键任务和关键业务用例中实现 Zero Trust 所需的灵活性、敏捷性和效率，可提供从关键基础架构和知识产权到用户身份和凭据的全面安全防护。Akamai 在网络基础架构、分段和微分段方面拥有丰富的经验，能够切实帮助企业规划、构建、部署乃至管理基于微分段工具和思维模式而构建的安全基础架构。

Enterprise Strategy Group 是一家综合性技术分析、研究和战略公司，为全球 IT 界提供市场情报、可行洞察和营销内容服务。

www.esg-global.com　　contact@esg-global.com　　508.482.0188